# CLAIMS

1. An anonymous electronic voting system comprising:

voter terminals (100, 110, 140) for receiving a list of combinations of candidate name and encrypted candidate name, to transmit said encrypted candidate name of a selected candidate via a network;

at least one encryption server (400, 410, 440) for receiving and re-encrypting said encrypted candidate name to create encrypted voting data, and returning said encrypted voting data to said voter terminal (100, 110, 140) having transmitted said encrypted candidate name;

a voting server (200) for receiving said encrypted voting data from said voter terminal (100, 110, 140) to create a list of effective encrypted voting data from among said received encrypted voting data, and transmitting said created list of said effective encrypted voting data via said network; and

a decryption server (500) for decrypting said list of said effective encrypted voting data received from said voting server (200), to create and transmit via said network a list of plaintext candidate names rearranged from said list of said effective encrypted voting data,

wherein said voting server (200) receives said list of said plaintext candidate names from said decryption server (500), to tally vote results based on said list of said received candidate

names.

2. The anonymous electronic voting system according to claim 1, further comprising another voter terminal (120, 130, 150) including an encryption means (124, 134, 154) for encrypting a candidate name of a selected candidate to create an encrypted candidate name.

3. The anonymous electronic voting system according to 1 or 2 further comprising an authentication server (300) including a storage device for storing a list of identification data of voters or voter terminals included in a voter list, said authentication server (300) receiving said encrypted voting data and identification data from said voter terminal (100, 110, 120, 130) to certify said encrypted voting data based on said identification data stored in said storage device, wherein said voting server (200) acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

4. The anonymous electronic voting system according to claim 1 or 2, further comprising an authentication server (300), wherein:

said voter terminal (110, 130) includes an intra-organization-signature creation means (113, 133) for creating

an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key,

said authentication server (300) receives said encrypted voting data, said intra-organization identification data, and said intra-organization digital signature from said voter terminal (110, 130), to certify said intra-organization digital signature based on a public key; and

said voting server (200) acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

5. The anonymous electronic voting system according to any one of claims 1 to 4, wherein said at least one encryption server include a group of encryption servers (400-1 to 400-k, 410-1 to 410-k, 440-1 to 440-k) for consecutively multiple-encrypting said encrypted candidate name, and said voting server (200) receives said encrypted voting data multiple-encrypted by said group of said encryption servers (400-1 to 400-k, 410-1 to 410-k, 440-1 to 440-k).

6. The anonymous electronic voting system according to claim 1 or 2, wherein:

each of said combinations in said list includes, in addition to said candidate name and said encrypted candidate

name, certificate data for certifying that said candidate name is legitimately encrypted; and

said encryption server (400, 410, 440) creates, in addition to said encrypted voting data, certificate data for certifying legitimacy of said encrypted voting data, to return the same to said voter terminal (100, 110, 140).

7. An anonymous electronic voting system comprising:

voter terminals (100, 110, 140) connected to a network;

a first encryption server (200) including a first data conversion means (206) for creating a first encryption parameter for each of said voter terminals (100, 110, 140) from public information, and transmitting said first parameter to said voter terminals (100, 110, 140);

a second encryption server (400, 410, 440) including a second data conversion means (405, 415, 445) for creating a second encryption parameter, and transmitting said second parameter to said voter terminals (100, 110, 140);

a voting server (200) for receiving encrypted voting data from said voter terminals (100, 110, 140) to create a list of effective encrypted voting data from among said received encrypted voting data, and transmitting said created list of said effective encrypted voting data via said network; and

a decryption server (500) for decrypting said list of said effective encrypted voting data received from said voting

server (200), to create and transmit via said network a list of plaintext candidate names rearranged from said list of said effective encrypted voting data, wherein:

said voting server (200) receives said list of said plaintext candidate names from said decryption server (500), to tally voted results based on said list of said received candidate names; and

said voter terminals (100, 110, 140) each include an encryption means (104, 114, 144) for encrypting voting contents based on said first and second encryption parameters to create encrypted voting data, and transmits said encrypted voting data to said voting server (200).

8. The anonymous electronic voting system according to claim 7, wherein said first encryption server (200) and said voting server (200) operate on a common server.

9. The anonymous electronic voting system according to claim 7 or 8, wherein:

said voter terminals (100, 110, 140) create, in addition to said encrypted voting data, encryption-certificate data, and transmits the same to said voting server (200);

said voting server (200), upon completing verification of legitimacy by verifying at least said encryption-certificate data, acknowledges corresponding said encrypted voting data as said

effective encrypted voting data.

10. The anonymous electronic voting system according to any one of claims 7 to 9, further comprising an authentication server (300) including a storage device for storing a list of identification data of voters or voter terminals included in a voter list, said authentication server (300) receiving said encrypted voting data and identification data from said voter terminals (100, 110, 120, 130) to certify said encrypted voting data based on said identification data stored in said storage device, wherein said voting server (200) acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

11. The anonymous electronic voting system according to any one of claims 7 to 9, further comprising an authentication server (300), wherein:

said voter terminals (110) each include an intra-organization-signature creation means (113) for creating an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key,

said authentication server (300) receives said encrypted voting data, said intra-organization identification data, and said intra-organization digital signature from said voter terminal

(110, 130), to certify said intra-organization digital signature based on a public key; and

said voting server (200) acknowledges at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.

12. An anonymous electronic voting method using a voting server, a voter terminal for voting therethrough by a voter, an encryption server, and a decryption server, said comprising the steps of:

transmitting from said voting server (200) a list of combinations of candidate name and encrypted candidate name obtained by encrypting said candidate name to said voter terminal (100, 110, 140) via a network;

transmitting from said voter terminal (100, 110, 40) an encrypted candidate name, which is paired with a candidate name selected by a voter, to said encryption server (400, 410, 440);

re-encrypting said encrypted candidate name in said encryption server (400, 410, 440) to create encrypted voting data, and transmitting said encrypted voting data to said voter terminal (100, 110, 140) having transmitted said encrypted candidate name;

transmitting from said voter terminal (100, 110, 140) said encrypted voting data, which is received from said encryption

server (400, 410, 44), to said voting server (200);

receiving said encrypted voting data in said voting server (200) to create and transmit a list of effective encrypted voting data;

decrypting said list of said encrypted voting data in said decryption server (500) to create a list of plaintext candidate names rearranged; and

receiving said list of said plaintext candidate names in said voting server (200) to tally vote results based on said list of said received candidate names.

13. The anonymous electronic voting method according to claim 12, further comprising the steps of:

receiving from said voter terminal (100) said encrypted voting data and identification data in an authentication server (300) to certify said encrypted voting data based on identification data stored in a storage device and transmitting said encrypted voting data; and

acknowledging in said voting server (200) at least said encrypted voting data affixed with certificate data by said authentication server (300) as said effective encrypted voting data.

14. The anonymous electronic voting method according to claim 12, further comprising the steps of:

creating in said voter terminal (110) an intra-organization-signature creation means (113, 133) for an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key;

acknowledging in said voting server (200) at least said encrypted voting data affixed with certificate data by said authentication server (300) as said effective encrypted voting data.

15. The anonymous electronic voting method according to claim 12, wherein said step of re-encrypting said encrypted candidate name is the step of consecutively multiple-encrypting said encrypted candidate name in a group of encryption servers (400-1 to 400-k, 410-1 to 410-k, 440-1 to 440-k).

16. The anonymous electronic voting method according to claim 12, wherein:

each of said combinations in said list includes, in addition to said candidate name and said encrypted candidate name, certificate data for certifying that said candidate name is legitimately encrypted; and

said encryption server (400, 410, 440) creates, in addition to said encrypted voting data, certificate data for certifying legitimacy of said encrypted voting data, to return the same to said voter terminal (100, 110, 140).

17. An anonymous electronic voting method comprising the steps of:

creating in a first encryption server (200) a first encryption parameter for each of voter terminals (100, 110, 140) from public information, and transmitting said first parameter to said voter terminals (100, 110, 140);

creating in a second encryption server (400, 410, 440) a second encryption parameter for each of said voter terminals (100, 110, 140) from said public information, and transmitting said second parameter to said voter terminals (100, 110, 140);

encrypting voting contents of a voter in said voter terminal (100, 110, 140) based on said first and second encryption parameters to create encrypted voting data, and transmitting said encrypted voting data to said voting server (200);

creating a list of effective encrypted voting data from among said received encrypted voting data in said voting server (200), and transmitting said created list of said effective encrypted voting data via said network;

decrypting in a decryption server (500) said list of said effective encrypted voting data received from said voting server (200), to create and transmit via said network a list of plaintext candidate names rearranged from said list of said effective encrypted voting data; and

receiving in said voting server (200) said plaintext candidate names, to tally voted results based on said list of said received candidate names.

18. The anonymous electronic voting method according to claim 17, wherein said encryption voting data creating step creates encryption-certificate data certifying legitimacy of said encrypted voting data, further comprising the step:

after verifying legitimacy in said voting server (200) by verifying at least said encryption-certificate data, acknowledging corresponding said encrypted voting data as said effective encrypted voting data.

19. The anonymous electronic voting method according to claim 17, further comprising the steps of: receiving in a certification server (300) said encrypted voting data and identification data from said voter terminal (100), and certifying said encrypted voting data based on identification data stored in a storage device; and acknowledging in said voting server (200) at least said encrypted voting data affixed with said certificate data as said effective voting data.

20. The anonymous electronic voting method according to claim 17, further comprising the steps of:

creating in said voter terminal (110) an intra-organization digital signature based on said encrypted voting data, intra-organization identification data, and a private key;

receiving in said authentication server (300) said encrypted voting data, said intra-organization identification data, and said intra-organization digital signature from said voter terminal (110), to certify said intra-organization digital signature based on a public key; and

acknowledging in said voting server (200) at least said encrypted voting data affixed with certificate data by said authentication server as said effective encrypted voting data.